

IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to said computing device through an interface;

determining whether or not resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

loading said available software into said storage device if said resident software has not been authenticated; and

setting an authentication flag if said available software is authenticated.

2. (Previously Presented) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to said computing device through an interface;

determining whether or not resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

loading said available software if said resident software is authenticated and said available software is authenticated.

3. (Currently Amended) The method of claim 2 wherein said determining whether or not said resident software is authenticated comprises of:

determining whether or not an authentication flag has been set;

wherein said resident software is determined to be authenticated if an ~~said~~ authentication flag has been set; otherwise

said resident software is determined to be unauthenticated.

4. (Previously Presented) The method of claim 3 wherein said authentication flag is set when said available software is determined to be authenticated.

5. (Currently Amended) The method of claim [3]~~4~~ wherein said authentication flag is set by a service technician.

6. (Previously Presented) The method of claim 2 wherein said determining whether or not said resident software is authenticated comprises of performing a direct authentication procedure on said resident software.

7. (Currently Amended) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

8. (Currently Amended) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

9. (Previously Presented) An apparatus for performing configuration management for a computing device, comprising:

- an interface for providing available software to be loaded into said computing device to said computing device;

- a storage device for storing resident software and a set of executable computer instructions for determining whether or not said available software and said resident software are authenticated;

- a processor for executing said set of executable computer instructions and for: loading said available software into said computing device if said resident software is not authenticated; and

- setting an authentication flag if said available software is authenticated.

10. (Previously Presented) An apparatus for performing configuration management for a computing device, comprising:

- an interface for providing available software to be loaded into said computing device to said computing device;

- a storage device for storing resident software and a set of executable computer instructions for determining whether or not said available software and said resident software are authenticated;

- a processor for executing said set of executable computer instructions and for:

- rejecting said available software if said resident software has been authenticated and said available software is not authenticated; and

loading said available software if said resident software is authenticated and said available software is authenticated.

11. (Previously Presented) The apparatus of claim 10 wherein:
said storage device is further for storing an authentication flag for indicating the authentication status of said computing device; and
said processor is further for determining whether or not said resident software is authenticated based on said authentication flag.

12. (Original) The apparatus of claim 11 wherein said authentication flag is set when authenticated software is loaded onto said computing device.

13. (Original) The apparatus of claim 11 wherein said authentication flag is set by a service technician.

14. (Previously Presented) The apparatus of claim 10 wherein said processor is further for performing a direct authentication procedure on said resident software to determine whether or not said resident software is authenticated.

15. (Currently Amended) The apparatus of claim 14 wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

16. (Currently Amended) The apparatus of claim 14 wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

17. (Previously Presented) An apparatus for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to said computing device through an interface;

means for determining whether or not resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for loading said available software into said storage device if said resident software has not been authenticated; and

means for setting an authentication flag if said available software is authenticated.

18. (Previously Presented) An apparatus for implementing a method for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to said computing device through an interface;

means for determining whether or not resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

means for loading said available software if said resident software is authenticated and said available software is authenticated.

19. (Previously Presented) A computer-readable medium embodying codes for implementing a method for configuration management for a computing device, the method comprising :

providing available software to be loaded into said computing device to said computing device through an interface;

determining whether or not resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

loading said available software into said storage device if said resident software has not been authenticated; and

setting an authentication flag if said available software is authenticated.

20. (Previously Presented) A computer-readable medium embodying codes for implementing a method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to said computing device through an interface;

determining whether or not resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said

available software is not authenticated; and

loading said available software if said resident software is authenticated and said available software is authenticated.